🧠 Ejercicio Práctico: Análisis Conceptual del Hacking Ético

🎯 Objetivo:

Evaluar la comprensión crítica y reflexiva de los principios, roles y responsabilidades que definen al hacker ético, mediante el análisis de un escenario realista.

📝 Instrucciones:

Lee atentamente el caso práctico y responde las preguntas de análisis conceptual que siguen. Justifica tus respuestas utilizando conceptos clave del hacking ético.

📄 Caso práctico: “Simulación sin permiso”

Una empresa contrata a un consultor en ciberseguridad para mejorar su infraestructura de seguridad. Durante la reunión inicial, el consultor sugiere hacer pruebas de penetración inmediatamente, sin firmar ningún acuerdo ni detallar el alcance de su trabajo.

El mismo día, ejecuta un escaneo de puertos en los servidores públicos de la empresa y encuentra vulnerabilidades que documenta en un archivo. Sin embargo, el informe es compartido por correo sin cifrar y sin aviso previo a los responsables de TI. Además, en su reporte, minimiza una falla crítica argumentando que “no es explotable fácilmente”.

🧩 Preguntas de análisis:

1. **¿Qué principios éticos del hacking ético han sido vulnerados en este caso?**
   (Menciona al menos 3 y explica por qué se incumplen)
   ✅ *Respuesta esperada:* Consentimiento y autorización, confidencialidad, transparencia.

---

2. **¿Qué riesgos legales o de reputación podrían generarse para la empresa por aceptar este tipo de prácticas?**
   (Considera leyes de protección de datos, normativas como el GDPR, etc.)

---

3. **¿Qué acciones debió realizar el consultor antes de iniciar cualquier actividad técnica?**
   (Menciona procedimientos, documentación, roles involucrados, etc.)

---

4. **¿Cuál es la diferencia entre este comportamiento y el que debe tener un hacker ético profesional?**
   (Haz una comparación basada en principios y buenas prácticas)

---

5. **¿Qué perfil profesional hubiera sido más adecuado para iniciar el proceso de evaluación de seguridad en este caso: auditor, analista o pentester? Justifica tu elección.**

🧾 Criterios de evaluación:

- Comprensión clara de los principios éticos.
- Capacidad de aplicar teoría a un caso práctico.
- Uso correcto de terminología profesional.
- Justificación crítica y argumentada de cada respuesta.

✅ Ejemplo de solución: Análisis Conceptual del Hacking Ético

🧩 Pregunta 1: ¿Qué principios éticos del hacking ético han sido vulnerados en este caso?

Respuesta:

1. **Consentimiento y Autorización:** El consultor realizó un escaneo sin firmar ningún acuerdo ni definir el alcance. Toda actividad debe contar con aprobación formal y documentada.

2. **Confidencialidad y Privacidad:** Al compartir un informe con vulnerabilidades críticas sin cifrado y sin coordinación, se pone en riesgo la seguridad de la información.

3. **Transparencia y Comunicación Efectiva:** El profesional minimizó una falla crítica en el informe, lo que va contra el deber de reportar hallazgos con claridad y honestidad.

🧩 Pregunta 2: ¿Qué riesgos legales o de reputación podrían generarse para la empresa por aceptar este tipo de prácticas?

Respuesta:

- **Riesgos legales:** La empresa podría incumplir normativas como el GDPR, ya que se manipularon datos e infraestructura sin consentimiento claro ni protección adecuada.

- **Reputación:** Si el informe se filtra o se explota la vulnerabilidad no reportada adecuadamente, la empresa puede sufrir pérdida de confianza de clientes y socios.

- **Responsabilidad compartida:** La empresa puede ser considerada negligente al permitir actividades no reguladas.

🧩 Pregunta 3: ¿Qué acciones debió realizar el consultor antes de iniciar cualquier actividad técnica?

Respuesta:

- Firmar un acuerdo formal que establezca los términos del servicio, incluyendo autorización escrita.
- Definir el **alcance**, metodología, tiempos, y objetivos del test.
- Coordinar con el equipo de TI y legal de la empresa.
- Configurar canales seguros para la entrega del informe (cifrado, acceso restringido).
- Solicitar consentimiento explícito por escrito.

🧩 Pregunta 4: ¿Cuál es la diferencia entre este comportamiento y el que debe tener un hacker ético profesional?

Respuesta:

El comportamiento del consultor fue **improvisado, poco ético y riesgoso**. En cambio, un hacker ético profesional:

- **Actúa con autorización previa**, documentada y consensuada.
- **Respeta la confidencialidad** de la información y usa canales seguros.
- **Informa con transparencia**, sin minimizar hallazgos.
- **Sigue buenas prácticas** reconocidas (como OWASP o NIST) y tiene en cuenta normas legales y éticas.

🧩 Pregunta 5: ¿Qué perfil profesional hubiera sido más adecuado para iniciar el proceso de evaluación de seguridad en este caso? Justifica tu elección.

Respuesta:

El auditor de seguridad informática hubiera sido el más adecuado para iniciar, ya que:

- Evalúa de forma integral las políticas, controles y procesos actuales.
- Su análisis inicial puede determinar si es necesario o no un test de penetración.

- Ayuda a alinear las evaluaciones con normas como ISO/IEC 27001, evitando riesgos legales y garantizando un marco seguro y ético para futuras pruebas técnicas.
